UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,979	10/16/2003	Shell S. Simpson	200209258-1	8115

22879   7590   05/31/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
SHAN, APRIL YING

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after t he mailing date of this communication, even if timely filed, may re duce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 March 2007</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-41 and 47</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-41 and 47</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>16 October 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-41 and 47 have been examined.

Election/Restrictions

2.   Applicant's election without traverse of electing Group I (Claims 1-41 and 47),

withdraw Group II (Claims 42-46) and Group III (Claim 48) in the reply filed on 6 April

2007 is acknowledged.

Claim Objections

3.   Claims 5, 9 and 15 are objected to under 37 CFR 1.75(c), as being of improper

dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s)

in proper dependent form, or rewrite the claim(s) in independent form.

As per **claim 5**, it is depended on claim 4. However, according to claim 4, "an

encryption key" is optional since claim 4 recites "where the print request includes one or

more of, a print item identifier... an encryption key....". But it appears to the examiner,

according to claim 5, "encryption key" must include in the print request.

As per **claims 9 and 15**, the Applicant recites public key and session key. It

appears to the examiner that there is no correlation between public key and session key

as recited in the claims. Please clarify. Further, in **claim 15**, it recites "decrypting a

session key associated with print item encrypted in the first enterprise where the

encryption is based, at least in part, on the public key..." is grammatically

incomprehensible. Is the Applicant meant encrypt session key with the public key?

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

5.   Claims 1-17, 47 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

As per **claim 1**, line 14 recites "…one or more encryption data…". It is not clear

whether this encryption data is encrypted data of the print request or the print item or

both or neither.

As per **claims 11 and 17**, "decrypting the print item in the image forming device"

is recited. However, claims 11 and 17 also recites, "encrypting the print item in the first

enterprise". How can an encryption service to decrypt a non-encrypted print item?

As per **claim 47**, "an encryption data" is recited on line 33 of page 33. It is not

clear whether this encryption data is same as or different from "encryption data" recited

on line 1 of page 33.

Any claim not specifically addressed, above, is being rejected as incorporating

the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 101

6.   35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

7.   Claims 1, 6-10, 17-26, 33, 37, and 39-40 are rejected under 35 U.S.C. 101

because the claimed invention is directed to non-statutory subject matter.

With respect to **claims 1, 18 and 37,** they are directed to a secure foreign

enterprise print system comprises logics. However, in accordance with Applicant's

specification in the par. [0019] of page 3, "Logic may also be fully embodied as

software". Therefore, it appears that the system would reasonably be interpreted by

one of ordinary skill in the art as software, per se. There is no element positively recited

as part of the system. As such, it believed that the apparatus of claims 1, 18 and 37 are

reasonably interpreted as functional descriptive material, per se.

With respect to **claims 17 and 33,** the "computer-readable medium" is recited. In

accordance with Applicant's specification on page 3, par. [0018], is carrier wave/pulse

or signal. This subject matter is not limited to that which falls within a statutory category

of invention because it is not limited to a process, machine, manufacture, or a

composition of matter. Instead, it includes a form of energy. Energy does not fall within

a statutory category since it is clearly not a series of steps or acts to constitute a

process, not a mechanical device or combination of mechanical devices to constitute a

machine, not a tangible physical article or object which is some form of matter to be a

product and constitute a manufacture, and not a composition of two or more substances

to constitute a composition of matter.

Any claim not specifically addressed, above, is being rejected as incorporating

the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

9.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
        obviousness or nonobviousness.

10.   This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

11.   Claims 1-7, 10-13, 16-24, 27-29 and 33-36 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Lamming et al. (U.S. Patent No. 6,922,725) in view of Slick

et al. (U.S. Patent No. 7,003,667).

As per **claim 1**, Lamming et al. discloses a secure foreign enterprise print

system, comprising:

a wireless telephonic logic ("Bridging the two networks 102 and 101 to form a

path of connectivity between the output device 106 and the document server 108 is a

mobile computing device 10.." – e.g. col. 7, lines 19-31 and "In bridging the two

networks 102 and 104, the mobile computing device 110 performs discovery functions

112, preparation functions 114, and control functions 117..." – e.g. col. 7, lines 41-52);

a wireless network communication logic configured to communicate a

print request to a wireless network web services provider via the wireless telephonic

logic (e.g. col. 4, lines 16-31 and e.g. col. 10, lines 33-44 and fig. 3), the print request

being related to a print item stored (e.g. col. 10, lines 45-55) in a first enterprise ("a

second network 104 ("Network B") – e.g. fig. 1 and col. 5, lines 45-46. Please note

Network B corresponds to Applicant's a first enterprise) and an image forming device

("output device 106" – e.g. fig. 1 and col. 6, lines 36-37. Please note output device

corresponds to Applicant's image forming device) located in a second enterprise ("a

first network 102 ("Network A") – e.g. fig. 1 and col. 5, line 44. Please note Network A

corresponds to Applicant's a second enterprise);

a discovery logic configured to identify the image forming device ("In bridging the

two networks 102 and 104, the mobile computing device 110 performs discovery

function 12...(b) discovers the output device 106..." – e.g. col. 7, lines 41-51 and col. 9,

lines 1-12);

an image forming device communication logic configured to communicate an image forming device data with the image forming device (e.g. fig. 3 and col. 8, lines 44-59).

Lamming et al. further discloses a logic configured to communicate one or more data with one or more of, image forming device and the wireless network web services provider in col. 12, lines 28-39, "At 326, the document at 324 now in output format is transmitted to the mobile computing device over the second wireless communication 122... Upon receipt of the rendered document from the document server, the mobile computing device relays the rendered document over the first wireless communications channel 120 to the output device 106 at 327..." and in col. 12, lines 40-50, "...the document server... and that this preparation and/or rendering... **certain transformations** of the document may take place... for example, performed for the purpose of compression, **security**, and/or efficiency..."

Lamming et al. does not expressly disclose data are encrypted.

However, this commonly known features in the art are disclosed in Slick et al., "Encryption/decryption logic 413 allows server 40 to receive encrypted data and to either maintain such data in queue 415 or to send such data to an image output device such as printer 50 for printing" – e.g. col. 9, lines 16-19 and "Encryption/decryption logic 355 enables printer 50 to receive encrypted data according to the present invention" – e.g. col. 8, lines 36-38"

It would have been obvious to a person with ordinary skill in the art to incorporate Slick et al.'s data encryption into Lamming et al.'s system.

The motivation of doing so would have been "...the document server... and that

this preparation and/or rendering...certain transformations of the document may take

place...for example, performed for the purpose of compression, security, and/or

efficiency..." as disclosed in Lamming et al. (col. 12, lines 40-50) and "desirable if such

an improved path for routing documents would provide increased security..." as

disclosed in Lamming et al. (col. 3, lines 65-67)

As per **claim 2**, Lamming et al. – Slick et al. discloses a system as applied above

in claim 1. Lamming et al. further discloses where the wireless telephonic logic

comprises a cellular telephone ("..a mobile computing device 110...mobile phones" –

e.g. fig. 1 and col. 7, lines 19-31).

As per **claims 3-5**, Lamming et al. – Slick et al. discloses a system as applied

above in claim 1. Lamming et al. - Slick et al. further discloses where the image

forming device comprises a printer (Lamming et al. - e.g. col. 6, lines 52-54), where the

print request includes one or more of, a print item identifier, a user identifier, an

encryption key, an image forming device model data, an image forming device

capability data, an image forming device address, and a print queue identifier ("The

document service request includes a first parameter identifying a document..and a

second parameter identifying a type of output device available..." – Lamming et al.,

e.g. abstract and col. 10, lines 18-24), and where the encryption key is the public key

component of a public/private key pair that includes a public key component and a

private key component (Slick et al., "The first key is then encrypted using a second key and a third key. The second key is a public key...." – e.g. abstract and "..The encryption of the key is performed by an asymmetric encryption (i.e., public/private key –pair) algorithm" – e.g. col. 1, lines 39-49).

As per **claim 6**, Lamming et al. – Slick et al. discloses a system as applied above in claim 1. Lamming et al. further discloses where the image forming device communication logic is configured to communicate with the image forming device using one or more of, an IEEE 802.11 communication, an IEEE 802.15 communication, an infrared communication, and a Bluetooth communication (e.g. col. 5, lines 52-53 and col. 23, lines 16-21).

As per **claim 7**, Lamming et al. – Slick et al. discloses a system as applied above in claim 1. Lamming et al. further discloses where the image forming device data includes one or more of, a printer request, an encrypted encryption key, a decrypted encryption key, a print item identifier, an image forming device model data, an image forming device capability data, an image forming device address, and a print queue identifier (e.g. col. 8, lines 47-59 and col. 9, lines 43-49).

As per **claim 10**, Lamming et al. – Slick et al. discloses a system as applied

above in claim 1. Lamming et al. further discloses comprising: a user interface logic

configured to facilitate selecting the print item from the first enterprise (e.g. fig. 3, fig. 5

and col. 8, lines 10-59).

As per **claim 11**, Lamming et al. discloses a method comprising:

receiving a print item identifier that identifies a print item to process ("The

document service request includes a first parameter identifying a document available to

the document server" – e.g. abstract), where the print item is stored in a first enterprise

("...the document from a storage device local to the document server 108..." – e.g. col.

10, lines 45-55, "Forming part of the second network 104 is a document server 108..."

– e.g. col. 6, lines 56-67. Please note second network 104 corresponds to Applicant's

first enterprise);

receiving an image forming device identifier that identifies an image

forming device on which the print item is to be processed, where the image forming

device ("output device 106" – e.g. fig. 1 and col. 6, lines 36-37. Please note output

device corresponds to Applicant's image forming device) is located in a second

enterprise ("a first network 102 ("Network A") – e.g. fig. 1 and col. 5, line 44. Please

note Network A corresponds to Applicant's a second enterprise);

providing a print request (e.g. col. 4, lines 16-31 and e.g. col. 10, lines 33-

44 and fig. 3) to a wireless network web services provider that has access to the first

enterprise ("a second network 104 ("Network B") – e.g. fig. 1 and col. 5, lines 45-46.

Please note Network B corresponds to Applicant's a first enterprise) and the second

enterprise ("a first network 102 ("Network A") – e.g. fig. 1 and col. 5, line 44. Please

note Network A corresponds to Applicant's a second enterprise); and

      Lamming et al. further discloses in col. 12, lines 28-39, "At 326, the

document at 324 now in output format is transmitted to the mobile computing device

over the second wireless communication 122...Upon receipt of the rendered document

from the document server, the mobile computing device relays the rendered document

over the first wireless communications channel 120 to the output device 106 at 327..."

and in col. 12, lines 40-50, "...the document server... and that this preparation and/or

rendering... **certain transformations** of the document may take place...for example,

performed for the purpose of compression, **security**, and/or efficiency..."

Lamming et al. does not expressly disclose "providing an encryption service that

facilitates encrypting the print item in the first enterprise.and decrypting the print item in

the image forming device".

Slick et al. discloses providing an encryption service that facilitates encrypting the

print item in the first enterprise and decrypting the print item in the image forming

device ("In a network environment, a print job generated by a computer at one location

in the network can be printed by an image output device at another location..." – e.g.

col. 1, lines 14-16 and "...by encrypting print data...Then, the encrypted print data and

the encrypted randomly generated key are sent to the image output device...the print

data is decrypted using the decrypted symmetric key, and an image is output by the

image output device in accordance with the decrypted print data" – e.g. col. 1, lines 39-58. Please note one location corresponds to Applicant's first enterprise).

It would have been obvious to a person with ordinary skill in the art to incorporate Slick et al.'s data encryption/decryption into Lamming et al.'s method.

The motivation of doing so would have been "...the document server... and that this preparation and/or rendering... **certain transformations** of the document may take place...for example, performed for the purpose of compression, **security**, and/or efficiency..." as disclosed in Lamming et al. (col. 12, lines 40-50), "desirable if such an improved path for routing documents would provide increased security..." as disclosed in Lamming et al. (col. 3, lines 65-67).

As per **claim 12**, Lamming et al. – Slick et al. discloses a method as applied above in claim 11. Lamming et al. further discloses where the image forming device identifier includes one or more of, an image forming device address, an image forming device capability data, and an image forming device model data (e.g. col. 8, lines 51-59).

As per **claim 13**, Lamming et al. – Slick et al. discloses a method as applied above in claim 11. Lamming et al. further discloses where the print request includes one or more of, a print item identifier, an encryption key, an image forming device model data, an image forming device address, an image forming device capability data, and a print queue identifier ("The document service request includes a first parameter identifying a document..and a second parameter identifying a type of output device available..." – e.g. abstract).

As per **claim 16**, Lamming et al. – Slick et al. discloses a method as applied

above in claim 11. Lamming et al. further discloses where the image forming device

comprises a printer (e.g. col. 6, lines 52-54).

As per **claim 17**, Lamming et al. – Slick et al. discloses a method as applied

above in claim 11. Therefore, Lamming et al. – Slick et al. discloses the claimed

processor executable instructions stored in a computer-readable medium for carrying

out the method of steps.

As per **claim 18**, Lamming et al. discloses an image forming system, comprising:

a network communication logic configured to communicate with a web

services provider (e.g. col. 18, lines 54-62, fig. 14);

a wireless communication device logic configured to communicate with a

wireless communication device (e.g. col. 4, lines 16-31 and e.g. col. 10, lines 33-44,

col. 18, lines 54-62, figs. 3 and 14) and to employ the web services provider for print

services associated with producing an image from a print item stored (e.g. col. 10, lines

45-55) in a first enterprise ("a second network 104 ("Network B") – e.g. fig. 1 and col. 5,

lines 45-46. Please note Network B corresponds to Applicant's a first enterprise),

where the image forming system (e.g. col. 7, lines 59-63 and output device 106 in fig.

2) is located in a second enterprise ("a first network 102 ("Network A") – e.g. fig. 1 and

col. 5, line 44. Please note Network A corresponds to Applicant's a second enterprise);

an image forming logic configured to produce the image from the print item (e.g.

col. 12, lines 53-61).

Lamming et al. further discloses a logic configured to facilitate providing security

for the print item as it is communicated from the first enterprise to the image forming

system via the web service provider in col. 12, lines 28-39, "At 326, the document at

324 now in output format is transmitted to the mobile computing device over the

second wireless communication 122... Upon receipt of the rendered document from the

document server, the mobile computing device relays the rendered document over the

first wireless communications channel 120 to the output device 106 at 327..." and in

col. 12, lines 40-50, "...the document server... and that this preparation and/or

rendering... **certain transformations** of the document may take place...for example,

performed for the purpose of compression, **security**, and/or efficiency..."

Lamming et al. does not expressly disclose log is an encryption logic.

However, this commonly known features in the art are disclosed in Slick et al.,

"Encryption/decryption logic 413 allows server 40 to receive encrypted data and to

either maintain such data in queue 415 or to send such data to an image output device

such as printer 50 for printing" – e.g. col. 9, lines 16-19 and "Encryption/decryption

logic 355 enables printer 50 to receive encrypted data according to the present

invention" – e.g. col. 8, lines 36-38"

It would have been obvious to a person with ordinary skill in the art to incorporate Slick et al.'s data encryption into Lamming et al.'s system.

The motivation of doing so would have been "...the document server... and that this preparation and/or rendering...certain transformations of the document may take place...for example, performed for the purpose of compression, security, and/or efficiency..." as disclosed in Lamming et al. (col. 12, lines 40-50) and "desirable if such an improved path for routing documents would provide increased security..." as disclosed in Lamming et al. (col. 3, lines 65-67)

As per **claim 19**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Lamming et al. further discloses where the network communication logic is configured to communicate via the public Internet (e.g. col. 18, lines 23-34).

As per **claim 20**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Slick et al. further discloses where the network communication logic is configured to request an encrypted print item from a print queue (queue 356 in fig. 3 and e.g. col. 8, lines 41-42) associated with the web services provider (e.g. col. 4, lines 33-37 and col. 11, lines 20-23)

As per **claim 21**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Slick et al. further discloses where the network communication logic is configured to receive an encrypted print item from a print queue associated with the

web services provider (e.g. col. 4, lines 33-37, col. 8, lines 26-30 and col. 8, lines 36-42).

As per **claims 22-23**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Lamming et al. – Slick et al. further discloses where the wireless communication device logic is configured to communicate an image forming device data with the wireless communication device (Lamming et al., fig. 3) and where the image forming device data includes one or more of, a printer request, an encrypted encryption key, a decrypted encryption key, a print item identifier, an image forming device model data, an image forming device capability data, an image forming device address, and a print queue identifier (Lamming et al. - e.g. col. 8, lines 47-59 and col. 9, lines 43-49 and Slick et al. – e.g. col. 1, lines 48-49).

As per **claim 24**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Lamming et al. further discloses where the wireless communication device logic communicates with the wireless communication device using one or more of an IEEE 802.11 communication, an IEEE 802.15 communication, an infrared communication, and a Bluetooth communication (e.g. col. 5, lines 52-53).

As per **claim 27**, Lamming et al. – Slick et al. discloses a system as applied above in claim 18. Lamming et al. further discloses where the image forming device is a printer (e.g. col. 6, lines 52-54).

As per **claim 28**, Lamming et al. – Slick et al. discloses a system as applied

above in claim 18. Lamming et al. further discloses where the wireless communication

device is a cellular telephone ("..a mobile computing device 110...mobile phones" –

e.g. fig. 1 and col. 7, lines 19-31).

As per **claim 29**, Lamming et al. discloses in (e.g. fig. 3 and col. 8, line 10- col.

12, line 61) a method, comprising:

receiving into an image forming device, from a wireless communication device, a

request to produce an image from print item stored in a print queue provided by a web

services provider; communicating with the web services provider to have the print item

transmitted to the image forming device; receiving the print item (e.g. fig. 3); and

forming an image from the print item.

Lamming et al. further discloses a logic configured to communicate one or more

data with one or more of, image forming device and the wireless network web services

provider in col. 12, lines 28-39, "At 326, the document at 324 now in output format is

transmitted to the mobile computing device over the second wireless communication

122...Upon receipt of the rendered document from the document server, the mobile

computing device relays the rendered document over the first wireless communications

channel 120 to the output device 106 at 327..." and in col. 12, lines 40-50, "...the

document server... and that this preparation and/or rendering... **certain**

transformations of the document may take place...for example, performed for the

purpose of compression, **security**, and/or efficiency..."

Lamming et al. does not expressly disclose data are encrypted/decrypted.

However, this commonly known features in the art are disclosed in Slick et al.,

"Encryption/decryption logic 413 allows server 40 to receive encrypted data and to

either maintain such data in queue 415 or to send such data to an image output device

such as printer 50 for printing" – e.g. col. 9, lines 16-19 and "Encryption/decryption

logic 355 enables printer 50 to receive encrypted data according to the present

invention" – e.g. col. 8, lines 36-38" and "...the print data is decrypted using the

decrypted symmetric key, and an image is output by the image output device in

accordance with the decrypted print data" – e.g. col. 1, lines 55-58.

It would have been obvious to a person with ordinary skill in the art to incorporate

Slick et al.'s data encryption/decryption into Lamming et al.'s system.

The motivation of doing so would have been "...the document server... and that

this preparation and/or rendering...certain transformations of the document may take

place...for example, performed for the purpose of compression, security, and/or

efficiency..." as disclosed in Lamming et al. (col. 12, lines 40-50) and "desirable if such

an improved path for routing documents would provide increased security..." as

disclosed in Lamming et al. (col. 3, lines 65-67)

As per **claims 33**, Lamming et al. – Slick et al. discloses a method as applied above in claim 29. Therefore, Lamming et al. – Slick et al. discloses the claimed processor executable instructions stored in a computer-readable medium for carrying out the method of steps.

As per **claim 34**, it is rejected using the same rationale as rejecting claims 1-3 above.

As per **claim 35**, Slick et al. further discloses where the network communication logic is configured to request an encrypted print item from a print queue associated with the web services provider (e.g. col. 4, lines 33-37 and col. 11, lines 20-23)

As per **claim 36**, Slick et al. further discloses where the network communication logic is configured to receive an encrypted print item from a print queue associated with the web services provider (e.g. col. 4, lines 33-37, col. 8, lines 26-30 and col. 8, lines 36-42).

12. Claims 8, 14, 25 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lamming et al. (U.S. Patent No. 6922725) in view of Slick et al. (U.S.

Patent No. 7003667), further in view of Strobel et al. (U.S. Patent No. 6751732) and

Lohstroh et al. (U.S. Patent No. 5768373).

As per **claims 8, 14, 25 and 31-32**, Lamming et al. – Slick et al. does not

expressly disclose generate a public/private key pair and to provide the public key to the

wireless network web services provider via the wireless network communication logic,

and to provide the private key to the image forming device via the image forming device

communication logic and to decrypt an encrypted print item received from the web

services provider based, at least in part, on the private key component of the one time

public/private key pair. However, Strobel et al. discloses generate a public/private key

pair and to provide the public key to the wireless network web services provider via the

wireless network communication logic, and to provide the private key to the image

forming device via the image forming device communication logic (e.g. col. 2, lines 49-

61, col. 3, lines 1-2, col. 4, line 49 - col. 5, line 31). It would have been obvious to a

person with ordinary skill in the art to add Storbel et al.'s feature into Lamming et al. –

Slick et al.' s system/method. The motivation of doing so would have been to use

"...well known data encryption and decryption...such as...public and private key

management", as disclosed by Storbel et al. (e.g. col. 4, line 50-54).

Lamming et al. – Slick et al. – Storbel et al. does not expressly disclose the

public/private key pair is a one-time public/private key pair. However, this well known

feature is disclosed in col. 5, lines 1-27 of the Lohstroh et al. reference. It would have

been obvious to a person with ordinary skill in the art to combine Lohstorh et al.'s one-

time public/private key pair into Lamming et al. – Slick et al. – Storbel et al.'s system.

The motivation of doing so would have been to enhance security by encrypt/decrypt

using public-key cryptography for only one particular communication session.

13.   Claims 9, 15, 26 and 30 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Lamming et al. (U.S. Patent No. 6922725) in view of Slick et al. (U.S.

Patent No. 7003667), further in view of Strobel et al (U.S. Patent No. 6751732)

As per **claims 9 and 15**, Lamming et al. – Slick et al. discloses a system/method

as applied above in claims 1 and 11. Slick et al. further discloses to decrypt an

encrypted session key associated with an encrypted print item into a decrypted session

key (Slick et al. – e.g. col. 1, lines 50-53), and to provide the decrypted session key to

the image forming device (Slick al. – e.g. col. 1, lines 54-58).

Lamming et al. – Slick et al. does not expressly discloses provide the public key

to the wireless network web services provider via the wireless network communication

logic.

Strobel et al. discloses provide the public key to the wireless network web

services provider via the wireless network communication logic (e.g. col. 2, lines 49-61,

col. 3, lines 1-2, col. 4, line 49 - col. 5, line 31). It would have been obvious to a person

with ordinary skill in the art to add Storbel et al.'s feature into Lamming et al. – Slick et

al.' s system/method. The motivation of doing so would have been to use "…well

known data encryption and decryption… such as… public and private key management",

as disclosed by Storbel et al. (e.g. col. 4, line 50-54).

As per **claims 26 and 30**, Lamming et al. – Slick et al. discloses a

system/method as applied above in claims 18 and 29. Slick et al. further discloses

where decrypting the encrypted print item comprises:

retrieving an encrypted session key from the encrypted print item (Slick et al. -

e.g. col. 17, lines 44-45);

decrypting the encrypted print item into the decrypted print item

based, at least in part, on the decrypted session key (Slick et al. – e.g. col. 17, lines 44-

47).

Lamming et al. – Slick et al. does not expressly disclose providing the key to the

wireless communication device for decryption receiving a session key from the wireless

communication device.

However, Strobel et al. discloses providing the key to the wireless

communication device for decryption receiving a key from the wireless communication

device (e.g. abstract, col. 2, lines 50-54, col. 3, lines 102 and col. 5, lines 4-31).

It would have been obvious to a person with ordinary skill in the art to incorporate

such well known features of Strobel et al.'s into Lamming et al. – Slick et al.'s

system/method.

The motivation of doing so would have been to "…can provide secure, on-

demand printing of documents…delivered to a printing device, thereby ensuring receipt

by the intended recipient and ensuring confidentiality of the contents of the document

or message", as disclosed by Strobel et al. (e.g. col. 2, lines 31-36)

14.   Claims 37-41 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Lamming et al. (U.S. Patent No. 6922725) in view of Slick et al. (U.S. Patent No.

7,003,667) and further in view of examiner's official notice.

As per **claim 37**, Lamming et al. discloses a secure foreign enterprise print

system, comprising:

a wireless network communication logic configured to communicate via cellular

telephony with one or more wireless communication devices (e.g. fig. 11 and col. 13,

lines 10-20);

a controller logic configured to receive a request (e.g. col. 4, lines 16-31 and e.g.

col. 10, lines 33-44 and fig. 3) to provide print services for a print item (e.g. col. 10,

lines 45-55) stored on a first enterprise ("a second network 104 ("Network B") – e.g.

fig. 1 and col. 5, lines 45-46. Please note Network B corresponds to Applicant's a first

enterprise) and, in response to receiving the request to provide print services,

generating a request for the print item, identifying a gateway (e.g. col. 13, lines 24-27

and col. 17, lines 39-45) to the first enterprise, and transmitting the request for the print

item to the gateway (e.g. col. 13, lines 24-27 and col. 17, lines 39-49);

➢ Lamming et al. does not expressly disclose data are encrypted.

However, this commonly known features in the art are disclosed in Slick et al.,

"Encryption/decryption logic 413 allows server 40 to receive encrypted data and to

either maintain such data in queue 415 or to send such data to an image output device

such as printer 50 for printing" – e.g. col. 9, lines 16-19 and "Encryption/decryption

logic 355 enables printer 50 to receive encrypted data according to the present

invention" – e.g. col. 8, lines 36-38"

It would have been obvious to a person with ordinary skill in the art to incorporate

Slick et al.'s data encryption into Lamming et al.'s system.

The motivation of doing so would have been "...the document server... and that

this preparation and/or rendering...certain transformations of the document may take

place...for example, performed for the purpose of compression, security, and/or

efficiency..." as disclosed in Lamming et al. (col. 12, lines 40-50) and "desirable if such

an improved path for routing documents would provide increased security..." as

disclosed in Lamming et al. (col. 3, lines 65-67)

Slick et al. further discloses a print queue data store configured to store

print items, and a print queue logic configured to receive a print item from the first

enterprise, to store the print item in the print queue data store, to receive a request for

the encrypted print item from an image forming device in a second enterprise, and to

transmit the encrypted print item to the image forming device (e.g. queue 356 in fig. 3,

col. 8, lines 26-30 and 36-42, e.g. col. 4, lines 33-37).

> Lamming et al. – Slick et al. does not disclose the print queue data store is

    organized, at least in part, on a per cellular telephone user basis.

However, the print queue data store is organized, at least in part,

on a per cellular telephone user basis is well known in the art at the time of the

invention. Therefore, the examiner takes official notice that one of ordinary skill in the

art would know print queue data store is organized, at least in part,

on a per cellular telephone user basis (for example, a wireless service provider's print

queue data store billing statements, call history and etc. is organized, at least in part, on

a per cellular telephone user basis). Therefore, it would have been obvious to one of

ordinary skill in the art at the time of the invention to add this well known feature

motivating by providing organization to the data.

As per **claim 38**, Lamming et al. further discloses where the one or more

wireless communication devices comprise cellular telephones ("..a mobile computing

device 110...mobile phones" – e.g. fig. 1 and col. 7, lines 19-31).

As per **claims 39 and 40**, Lamming et al. further comprising: an enterprise

gateway relationship data store configured to store data that relates a wireless

communication device user with an enterprise gateway; and where the controller

logic is configured to identify the gateway to the first enterprise based, at

least in part, on data stored in the enterprise gateway relationship data

store (e.g. col. 17, lines 39-49) and where the enterprise gateway relationship data

store comprises a table (e.g. col. 15, lines 46-60).

As per **claim 41**, it is rejected using the same rationale as rejecting claims 1-3,

18-22, 34-36 above except for the print queue data store is organized, at least in part,

on a per cellular telephone user basis.

However, the print queue data store is organized, at least in part,

on a per cellular telephone user basis is well known in the art at the time of the

invention. Therefore, the examiner takes official notice that one of ordinary skill in the

art would know print queue data store is organized, at least in part,

on a per cellular telephone user basis (for example, a wireless service provider's print

queue data store billing statements, call history and etc. is organized, at least in part, on

a per cellular telephone user basis). Therefore, it would have been obvious to one of

ordinary skill in the art at the time of the invention to add this well known feature

motivating by providing organization to the data.

As per **claim 47**, it is rejected using the same rationale as rejecting claims 1-3,

18-22, 34-36 above except for

➢ the print queue data store is organized, at least in part,

on a per cellular telephone user basis

However, the print queue data store is organized, at least in part,

on a per cellular telephone user basis is well known in the art at the time of the

invention. Therefore, the examiner takes official notice that one of ordinary skill in the

art would know print queue data store is organized, at least in part,

on a per cellular telephone user basis (for example, a wireless service provider's print

queue data store billing statements, call history and etc. is organized, at least in part, on

a per cellular telephone user basis). Therefore, it would have been obvious to one of

ordinary skill in the art at the time of the invention to add this well known feature

motivating by providing organization to the data.

the request for a print item includes a print item

> where the request for a print item includes an encryption data

However, a request includes an encryption data is well known in the art at

the time of the invention. Therefore, the examiner takes official notice that one of

ordinary skill in the art would know a request includes an encryption data.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of

the invention to add this well known feature motivating by providing security to the

data.

Conclusion

15.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. In particular, reference Clough et al. (U.S. Patent No. 6,912,374)

and Wiegley (U.S. Patent No. 6,711,677) disclose secure printing. Applicant is

strongly urged to review these references in response to the current office action.

Contact Information

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to April Y. Shan whose telephone number is (571) 270-
1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00
p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for
the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
USPTO Customer Service Representative or access to the automated information
system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

23 May 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100